

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

Satoshi HOSHINO  
Filed 6/9/00  
Q 59623

#2' off  
1c511 U.S. Pff  
09/590686  
06/09/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 6月10日

出 願 番 号

Application Number:

平成11年特許願第164179号

出 願 人

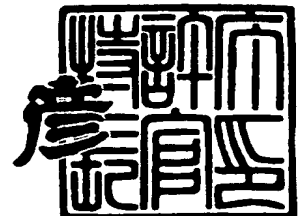
Applicant(s):

甲府日本電気株式会社

2000年 3月17日

特 許 庁 長 官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3017078

【書類名】 特許願

【整理番号】 03904964

【提出日】 平成11年 6月10日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 山梨県甲府市大津町 1 0 8 8 - 3 甲府日本電気株式会社  
社内

【氏名】 星野 聡

【特許出願人】

【識別番号】 000168285

【氏名又は名称】 甲府日本電気株式会社

【代理人】

【識別番号】 100104916

【弁理士】

【氏名又は名称】 古溝 聡

【選任した代理人】

【識別番号】 100095407

【弁理士】

【氏名又は名称】 木村 満

【手数料の表示】

【予納台帳番号】 073679

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9901051

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子データ管理装置、方法及び記録媒体

【特許請求の範囲】

【請求項 1】

電子データを入力するデータ入力手段と、  
前記データ入力手段から入力された情報を記録する電子データ記録手段と、  
着脱可能に構成された記録媒体が装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証手段と、  
特定人により操作されていることを認証する特定人認証手段と、  
前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可手段と、  
前記修正許可手段によって修正データの入力が許可されたときに、修正データを入力する修正データ入力手段と、  
前記修正データ入力手段から入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正手段と、  
前記データ入力手段からの電子データの入力の履歴と前記修正データ入力手段からの修正データの入力の履歴とを記憶管理する履歴管理手段と、  
を備えることを特徴とする電子データ管理装置。

【請求項 2】

前記履歴管理手段に記憶管理させるデータの入力の履歴を暗号化する手段をさらに備える

ことを特徴とする請求項 1 に記載の電子データ管理装置。

【請求項 3】

前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶管理されているデータの入力の履歴を復号化する手段をさらに備え、

前記修正許可手段は、復号化されたデータの入力の履歴を出力し、外部に提示することによって前記電子データ記録手段に記録されている電子データの修正を

許可し、

前記修正データ入力手段は、該出力されたデータの输入の履歴に基づいて、修正データを入力する

ことを特徴とする請求項 2 に記載の電子データ管理装置。

【請求項 4】

前記データ情報入力手段は、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力手段は、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録手段は、電子データまたは修正データを入力した者の認証情報を、入力された電子データまたは修正された電子データに対応付けて記録する

ことを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の電子データ管理装置

【請求項 5】

特定人の身体的特徴に関するデータを記憶する身体的特徴データ記憶手段をさらに備え、

前記特定人認証手段は、前記身体的特徴データ記憶手段に記憶されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行う

ことを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の電子データ管理装置

【請求項 6】

前記記録媒体は、特定人の身体的特徴に関するデータを記録しており、

前記特定人認証手段は、さらに前記記録媒体に記録されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行う

ことを特徴とする請求項 5 に記載の電子データ管理装置。

【請求項 7】

前記電子データ記録手段には、前記データ入力手段から電子データの入力がある都度、入力された電子データが記録される

ことを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載の電子データ管理装置

【請求項 8】

前記電子データ記録手段には、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶されている電子データの入力の履歴に基づいて、入力された電子データが記録される

ことを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載の電子データ管理装置

【請求項 9】

前記電子データ記録手段は、電子帳簿を記録するものであり、

前記電子データ及び前記修正データは、それぞれ電子帳簿に記録すべき取引に関する情報、該取引に関する情報を修正するための情報である

ことを特徴とする請求項 1 乃至 8 のいずれか 1 項に記載の電子データ管理装置

【請求項 10】

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおける電子データ管理方法であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第 1 の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第2の履歴管理ステップと、

を含むことを特徴とする電子データ管理方法。

【請求項 11】

前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させ、

前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させる

ことを特徴とする請求項 10 に記載の電子データ管理方法。

【請求項 12】

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおいて電子データを管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第 1 の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第 2 の履歴管理ステップと、

を実行するためのプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

### 【請求項 1 3】

前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させ、

前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させる

ことを特徴とする請求項 1 2 に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、特に電子帳簿の管理に好適な電子データ管理装置、方法及びコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】

取り引きに関する帳簿書類は、法律によって一定の期間保存することが義務づけられている。そして、平成11年1月からデータを電子化した電子帳簿として、帳簿書類を保存することが認められるようになった。このような電子帳簿については、脱税、背任といった重大な犯罪行為を防止するために、通常の電子データに比べて不正アクセスに対する非常に高いセキュリティを達成することが要請されている。

【0003】

【発明が解決しようとする課題】

これに対して、従来、一般的な電子データの管理方法として管理者の認証のために使用されているのは、パスワードである場合が多かった。パスワードによる認証では、パスワードが盗み出されてしまえば、誰でも管理対象としている電子データにアクセスすることができてしまう。このため、単純なパスワードでの認証による電子データの管理方法は、高度なセキュリティが要請される電子帳簿の管理に適用するのには適していなかった。

【0004】

本発明は、上記従来技術の問題点を解消するためになされたものであり、電子帳簿などの電子データの管理について、高いセキュリティを達成することができる電子データ管理装置、方法及び電子データ管理のためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成するため、本発明の第1の観点にかかる電子データ管理装置は



電子データを入力するデータ入力手段と、  
前記データ入力手段から入力された情報を記録する電子データ記録手段と、  
着脱可能に構成された記録媒体が装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証手段と、  
特定人により操作されていることを認証する特定人認証手段と、  
前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可手段と、  
前記修正許可手段によって修正データの入力が許可されたときに、修正データを入力する修正データ入力手段と、  
前記修正データ入力手段から入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正手段と、  
前記データ入力手段からの電子データの入力の履歴と前記修正データ入力手段からの修正データの入力の履歴とを記憶管理する履歴管理手段と、  
を備えることを特徴とする。

【0006】

上記電子データ管理装置は、前記履歴管理手段に記憶管理させるデータの入力の履歴を暗号化する手段をさらに備えるものとしてもよい。

【0007】

このような暗号化の手段を備える場合において、上記電子データ管理装置は、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶管理されているデータの入力の履歴を復号化する手段をさらに備えるものとしてもよい。この場合、前記修正許可手段は、復号化されたデータの入力の履歴を出力し、外部に提示することによって前記電子データ記録手段に記録されている電子データの修正を許可し、前記修正データ入力手段は、該出力されたデータの入力の履歴に基づいて、修正データを入力するものとしてすることができる。

【0008】

上記電子データ入力装置において、前記データ情報入力手段は、電子データを入力した者の認証情報を併せて入力するものとし、前記修正データ入力手段は、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録手段は、電子データまたは修正データを入力した者の認証情報を、入力された電子データまたは修正された電子データに対応付けて記録するものとすることができる。

## 【0009】

上記電子データ管理装置は、また、特定人の身体的特徴に関するデータを記憶する身体的特徴データ記憶手段をさらに備えるものとしてもよい。この場合、前記特定人認証手段は、前記身体的特徴データ記憶手段に記憶されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行うものとすることができる。

## 【0010】

さらに、前記記録媒体が、特定人の身体的特徴に関するデータを記録しているもよい。この場合、前記特定人認証手段は、さらに前記記録媒体に記録されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行うものとすることができる。

## 【0011】

上記電子データ管理装置において、前記電子データ記録手段には、前記データ入力手段から電子データの入力がある都度、入力された電子データが記録されるものとすることができる。

## 【0012】

また、前記電子データ記録手段には、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶されている電子データの入力の履歴に基づいて、入力された電子データが記録されるものとすることもできる。

## 【0013】

なお、上記電子データ管理装置において、前記電子データ記録手段は、電子帳簿を記録するものであることを好適とする。この場合には、前記電子データ及び

前記修正データは、それぞれ電子帳簿に記録すべき取引に関する情報、該取引に関する情報を修正するための情報とすることができる。

【 0 0 1 4 】

上記目的を達成するため、本発明の第 2 の観点にかかる電子データ管理方法は

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおける電子データ管理方法であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第 1 の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第 2 の履歴管理ステップと、

を含むことを特徴とする。

【 0 0 1 5 】

上記電子データ管理方法において、前記データ情報入力ステップは、電子デー

タを入力した者の認証情報を併せて入力するものとし、前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができ、前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができる。

【0016】

上記目的を達成するため、本発明の第3の観点にかかるコンピュータ読み取り可能な記録媒体は、

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおいて電子データを管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第1の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子デー

タ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第 2 の履歴管理ステップと、

を実行するためのプログラムを記録することを特徴とする。

【0 0 1 7】

上記コンピュータ読み取り可能な記録されたプログラムにおいて、前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものとし、前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができ、前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができる。

【0 0 1 8】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態について説明する。

【0 0 1 9】

図 1 は、この実施の形態にかかる電子帳簿管理システムの構成を示すブロック図である。図示するように、このシステムは、入力装置 1 8 及び出力装置 1 9 が接続された電子帳簿管理装置 1 と、これに着脱可能に構成された磁気カード 2 及び I C (Integrated Circuit) カード 4 を備える。また、このシステムは、後述する管理者の身体的特徴としての指紋 3 のデータを取り込むようになっている。

【0 0 2 0】

磁気カード 2 は、このシステムのユーザ、すなわち取り引き情報の書き込みを行う者によって所有され、磁気カードリーダー 1 1 へ挿入されたときにユーザによる取り引き情報の入力が可能となる。I C カード 4 は、このシステムの管理者によって所有され、I C カードリーダー/ライト 1 4 へ挿入されたときに管理者による取り引き情報の修正、削除が可能となる。なお、I C カード 4 には、管理者の

指紋のデータと所定の暗号鍵が予め記憶されている。

【0021】

電子帳簿管理装置 1 は、専用のコンピュータ装置、またはカスタマイズされた汎用のコンピュータ装置によって構成され、CPU (Central Processing Unit) 10a を含む制御部 10 と、磁気カードリーダー 11 と、指紋認証装置 12 と、指紋ファイル 13 と、IC カードリーダー/ライター 14 と、SAM (Secure Application Module) 15 と、電子帳簿ファイル 16 と、履歴管理ファイル 17 とを備えている。

【0022】

制御部 10 は、入力装置 18 からの入力に従って CPU 10a が内部メモリ 10b に記憶されている後述するフローチャートに示すプログラムを実行することにより、磁気カードリーダー 11、指紋認証装置 12、IC カードリーダー/ライター 14 及び SAM 15 の動作を制御し、或いは電子帳簿ファイル 16 及び履歴管理ファイル 17 の内容を更新する。制御部 10 は、また、所定の場合においてその処理結果を出力装置 19 に出力する。なお、制御部 10 は、履歴管理ファイル 17 への履歴記録のためのタイマを有している。

【0023】

磁気カードリーダー 11 は、磁気カード 2 が挿入された場合に、当該磁気カード 2 に書き込まれているデータを読み出す。磁気カードリーダー 11 は、読み出したデータにより、挿入された磁気カード 2 がユーザのものであるときには、その旨を制御部 10 に通知する。

【0024】

指紋認証装置 12 は、指紋 3 を読み取るスキャナと、読み取った指紋 3 のデータを、指紋ファイル 13 に記録されている指紋のデータ及び IC カード 4 から読み取られた指紋のデータとパターンマッチングする手段とを備える。指紋認証装置 12 は、パターンマッチングによりすべての指紋のデータが一致したときに、読み取られた指紋 3 が管理者のものであると認証し、その結果を制御部 10 に通知する。

【0025】

指紋ファイル 1 3 は、電子帳簿管理装置 1 内部の固定ディスク装置などに記憶され、予め指紋認証装置 1 2 のスキャナから読み込まれた電子帳簿管理装置 1 の管理者（1 人または複数人）の指紋 3 のデータを記録する。なお、指紋ファイル 1 3 は、内容の改竄を防ぐために、I C カードリーダー/ライター 1 4 に装着された I C カード 4 が正当なものであるとの機器認証が得られた場合のみに、アクセス可能にしてもよい。

【0 0 2 6】

I C カードリーダー/ライター 1 4 は、I C カード 4 が挿入された場合に、当該 I C カード 4 に記録されているデータを読み出す。I C カードリード/ライト 1 4 は、S A M 1 5 との間で後述するような機器認証を行い、機器認証が得られたときにはその旨を制御部 1 0 に通知する。なお、I C カードリード/ライト 1 4 は、I C カード 4 へ指紋のデータ及び暗号鍵を書き込むために使用してもよい。

【0 0 2 7】

S A M 1 5 は、例えば、1 チップの半導体装置によって構成され、暗号鍵（秘密鍵及び公開鍵）を格納している。S A M 1 5 及び I C カードリード/ライト 1 4 は、I C カードリード/ライト 1 4 に I C カード 4 が挿入されたときに、内部に格納している暗号鍵と I C カード 4 に記録されている暗号鍵とによるチャレンジレスポンスの手法を用いて、機器認証を行う。

【0 0 2 8】

電子帳簿ファイル 1 6 は、M O、C D - R、D V D などの電子帳簿管理装置 1 から着脱可能に構成された読み書き可能な記録媒体に記憶され、図 2 に示すように、取引に関する情報とその情報を入力した者の電子署名とをそれぞれ対応付けて記録する。なお、電子帳簿ファイル 1 6 へのデータの記録は、取り引きの発生の都度行われるか、或いは履歴管理ファイル 1 7 に蓄積された情報に基づいて一括して行われる。

【0 0 2 9】

履歴管理ファイル 1 7 は、電子帳簿管理装置 1 内部の固定ディスク装置などに記憶され、取引に関する情報及びその修正（削除を含む。以下、同じ）に関する情報を記録する。履歴管理ファイル 1 7 に記録される情報は、図 3 に示すように

、日付、時間、利用者、利用内容、金額、正常終了フラグ、修正フラグ及び修正内容の各項目からなる。

【0030】

履歴管理ファイル17は、ユーザが入力した取引に関する情報の履歴、管理者が修正した取引に関する情報の履歴を、その入力、修正の都度記録していく。なお、履歴管理ファイル17に記録されるデータは、すべてSAM15に格納されている公開鍵によって暗号化されており、管理者が修正を行う場合にのみ、SAM15に格納されている秘密鍵で復号化される。

【0031】

入力装置18は、キーボードなどによって構成され、ユーザまたは管理者が取引情報を入力したり、処理を選択したりするために用いられる。出力装置19は、ディスプレイ装置などによって構成され、制御部10による処理結果のうちの所定のもの、例えば、管理者が電子帳簿ファイル16を更新するときに復号化された履歴管理ファイル17を出力する。

【0032】

以下、この電子帳簿管理システムによる電子帳簿ファイル16の管理方法について説明する。ここでは、取引の都度、電子帳簿ファイル16へ取引に関する情報が書き込まれるものとする。また、このシステムでの電子帳簿ファイル16の管理が開始する前に、管理者の指紋3のデータを指紋ファイル13及び管理者が所有するICカード4に予め書き込まれているものとする。

【0033】

図4は、ユーザによる取引情報の入力の処理を示すフローチャートである。このフローチャートの処理は、ユーザによって磁気カード2が磁気カードリーダー11に挿入され、その磁気カード2がユーザのものであることが制御部10に通知されたときに開始する。

【0034】

まず、ユーザは、入力装置18から行った取引に関する情報と共に、当該ユーザの電子署名を入力する（ステップS11）。すると、制御部10は、内部タイマが示している日付、時刻、利用者名を入力された取引に関する情報及



び電子署名に付加する。さらに、制御部 1 0 は、S A M 1 5 に格納されている公開鍵を取り出し、この公開鍵で取り引きに関する情報等を暗号化して、履歴管理ファイル 1 7 へ記録する（ステップ S 1 2）。

【0 0 3 5】

次に、制御部 1 0 は、ステップ S 1 1 で入力された取り引きに関する情報及びユーザの電子署名を対応付けて、電子帳簿ファイル 1 6 へ記録する（ステップ S 1 6）。そして、このフローチャートの処理を終了する。

【0 0 3 6】

図 5 は、管理者による取り引き情報の修正の処理を示すフローチャートである。このフローチャートの処理は、管理者によって I C カード 4 が I C カードリード／ライト 1 4 に挿入されたときに開始する。

【0 0 3 7】

まず、I C カードリード／ライト 1 4 及び S A M 1 5 は、挿入された I C カード 4 に格納されている暗号鍵と S A M 1 5 に格納されている暗号鍵によるチャレンジレスポンスによって、挿入された I C カード 4 が正当なものであるかどうかの機器認証を行う（ステップ S 2 1）。そして、制御部 1 0 は、I C カードリード／ライト 1 4 からの通知に従って、機器認証が得られたかどうかを判定する（ステップ S 2 2）。

【0 0 3 8】

機器認証が得られたと判定した場合、制御部 1 0 は、指紋認証装置 1 2 に指紋 3 の照合を行わせる。この指紋の照合は、まず、指紋認証装置 1 2 のスキャナで指紋 3 のデータを読み取り、これを I C カードリード／ライト 1 4 で I C カード 4 から読み出した指紋のデータとパターンマッチングし、さらに、指紋ファイル 1 3 に記録されている指紋のデータとパターンマッチングし、すべてが一致するかどうかを比較することによって行う（ステップ S 2 3）。そして、制御部 1 0 は、指紋認証装置 1 2 からの通知に従って、指紋のデータが一致していたかどうかを判定する（ステップ S 2 4）。

【0 0 3 9】

指紋のデータが一致していたと判定した場合、制御部 1 0 は、S A M 1 5 に格

納されている秘密鍵を取り出し、この秘密鍵を用いて履歴管理ファイル 17 に格納されているデータを復号化する。そして、制御部 10 は、復号化した履歴管理ファイル 17 の内容を出力装置 19 に出力する（ステップ S25）。次に、管理者は、出力装置 19 から出力された履歴管理ファイル 17 のデータに従って、修正後のデータを、当該管理者の電子署名と共に入力装置 18 から入力する（ステップ S26）。

【0040】

制御部 10 は、内部タイマが示している日付、時刻、利用者名を入力された修正後のデータ及び電子署名に付加する。さらに、制御部 10 は、SAM15 に格納されている公開鍵を取り出し、この公開鍵で修正後のデータ等を暗号化して、履歴管理ファイル 17 へ記録する（ステップ S27）。次に、制御部 10 は、ステップ S27 で入力された修正後のデータに従って、電子帳簿ファイル 16 に記録されているデータを更新し、それと共に入力された電子署名を記録させる（ステップ S28）。そして、このフローチャートの処理を終了する。

【0041】

一方、ステップ S22 で機器認証が得られなかったと判定された場合、及びステップ S24 で指紋 3 のデータが一致しなかったと判定された場合には、そのままこのフローチャートの処理を終了する。

【0042】

以下、この実施の形態にかかる電子帳簿管理システムで行っているセキュリティ達成のための手段について、（１）～（４）に列記して分かり易く示す。

【0043】

（１）電子帳簿ファイル 16 へ記録されているデータを修正するためには、ＩＣカード 4 による機器認証と、指紋 3 による管理者の本人認証との双方が得られなければならない。このため、単純なパスワードによる認証等に比べると、システムの管理者以外の者が電子帳簿ファイル 16 へ記録されているデータを修正することができるようになる可能性が、非常に低くなる。

【0044】

（２）管理者の指紋 3 のデータのパターンマッチングを、指紋ファイル 13 に登

録されている指紋のデータと I C カード 4 に記録されている指紋のデータとの両方で行っている。このため、指紋ファイル 1 3 に記録されているデータが改竄されたり、I C カード 4 が偽造されたれたりしただけで、その両方がされない限り、電子帳簿ファイル 1 7 に記録されている情報を修正することができない。

【 0 0 4 5 】

( 3 ) 電子帳簿ファイル 1 6 へ記録している取引に関する情報には、それぞれ入力または修正を行ったものの電子署名が付されている。このため、誰が電子帳簿ファイル 1 6 に記録されている取引に関する情報の入力を行ったか、或いは修正を行ったかが一目瞭然となり、電子帳簿ファイル 1 6 に記録されているデータの正当性が確保される。

【 0 0 4 6 】

( 4 ) 履歴管理ファイル 1 7 へ取引に関する情報の入力、修正の履歴を記録する場合には、S A M 1 5 に格納されている公開鍵を利用して暗号化を行っている。そして、履歴管理ファイル 1 7 に記録されている履歴が復号化されるのは、I C カード 4 の機器認証、指紋 3 の認証の双方が得られた場合だけである。このため、システムの管理者以外の者によって履歴管理ファイル 1 7 に記録されているデータが不正に読み出されてしまうことがない。

【 0 0 4 7 】

すなわち、この実施の形態にかかる電子帳簿管理システムでは、予め登録した管理者以外の者が電子帳簿ファイル 1 6 にアクセスできる可能性が極端に低くなり、電子帳簿ファイル 1 6 の管理に対して高度なセキュリティを達成することが可能となる。また、履歴管理ファイル 1 7 の記録内容を読み出すことも難しくなり、高度なセキュリティを達成することができる。

【 0 0 4 8 】

本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について、説明する。

【 0 0 4 9 】

上記の実施の形態では、管理者を認証するための身体的特徴として、指紋 3 によるものとしていた。しかしながら、管理者という認証を得るための身体的特徴

としては、指紋 3 以外の他の身体的特徴、例えば、虹彩、手形、顔、声、網膜などのを適用することもできる。また、ICカード 4 による機器認証と共に、このような身体的特徴に加えて、或いはこれに代えて、パスワードによって管理者本人を認証するものとしてもよい。

#### 【0050】

上記の実施の形態では、電子帳簿管理システムの動作例として、取り引きに関する情報が入力される都度、その情報が電子帳簿ファイル 16 へ記録される者としていた。しかしながら、電子帳簿ファイル 16 への記録は、管理者のみが行えるものとしてもよい。この場合、図 4 のフローチャートの処理は、ステップ S 13 がなくなり、ステップ S 12 の処理で終了することとなる。

#### 【0051】

また、このような場合において管理者が IC カード 4 を IC カードリーダ/ライター 14 に挿入したときに実行される処理を、図 6 のフローチャートに示す。最初に図 5 のステップ S 21～S 24 の処理が行われる（ステップ S 31）。次に、管理者は、入力装置 18 を操作することによって、取り引きに関する情報の修正か、新たな記録かのいずれかの処理を選択する（ステップ S 32）。制御部 10 は、選択された処理が取り引きに関する情報の修正か、それとも記録であるかを判定する（ステップ S 33）。

#### 【0052】

選択された処理が修正であった場合には、図 5 のステップ S 25～S 28 の処理が行われ（ステップ S 34）、このフローチャートの処理を終了する。選択された処理が記録であった場合には、制御部 10 は、SAM 15 に格納されている秘密鍵を取り出し、履歴管理ファイル 17 に記録されているデータを復号化する。そして、制御部 10 は、復号化したデータのうちでまだ電子帳簿ファイル 16 に記録されていないものを電子帳簿ファイル 16 に記録する（ステップ S 35）。そして、このフローチャートの処理を終了する。

#### 【0053】

上記した図 6 のフローチャートに示す処理によることで、電子帳簿ファイル 16 に取り引きに関する情報を記録する場合には、管理者が必ず介在することにな

る。このため、この変形例での管理方法によることで、上記の実施の形態の管理方法よりも、電子帳簿ファイル 16 へのアクセスに対してさらに高度なセキュリティを達成することができるようになる。

【0054】

上記の実施の形態では、電子帳簿ファイル 16 及びその履歴管理ファイル 17 の管理に本発明を適用した場合を例として説明した。しかしながら、本発明は、電子帳簿以外の電子データ、特に電子帳簿と同程度にデータの盗用や改竄からの保護の要請が高い電子データの管理について、適用することができる。

【0055】

上記の実施の形態では、図 4、図 5 のフローチャートに示すプログラム（または、変形例で示した図 6 のフローチャートに示すプログラム）は、制御部 10 の内部メモリ 10b に記憶されているものとし、CPU 10a がこれを実行するものとしていた。

【0056】

しかしながら、このようなプログラムは、図 7 (a) に示すように、コンピュータ読み取り可能な記録媒体として、例えば MO 51 に格納し、MO ドライブ 50 で読み取って制御部 10 の内部メモリ 10b に記憶させるものとしてもよい。或いは、図 7 (b) に示すように、このようなプログラムをサーバ 62 に蓄積させておき、通信装置 60 からネットワーク 61 を介してサーバ 62 に要求を行い、サーバ 62 に蓄積されているプログラムを搬送波に重畳させたプログラムデータ信号をネットワーク 61 を介して通信装置 60 が受け取り、制御部 10 の内部メモリ 10b に記憶させるものとしてもよい。なお、図 7 (a)、(b) において図示しない他の構成は、図 1 に示すものと同じである。

【0057】

【発明の効果】

以上説明したように、本発明によれば、電子帳簿などの電子データの管理について、高度なセキュリティを達成することができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態にかかる電子帳簿管理システムの構成を示すブロック図である。

【図 2】

図 1 の電子帳簿ファイルに記録されるデータを示す図である。

【図 3】

図 1 の履歴管理ファイルに記録されるデータを示す図である。

【図 4】

ユーザが取り引き情報を入力するときの処理を示すフローチャートである。

【図 5】

管理者が取り引き情報を変更するときの処理を示すフローチャートである。

【図 6】

電子帳簿ファイルへの記録がすべて管理者によって行われる場合の処理を示すフローチャートである。

【図 7】

(a)、(b) は、本発明の実施の形態の変形例にかかる電子帳簿管理システムの簡略化した構成を示すブロック図である。

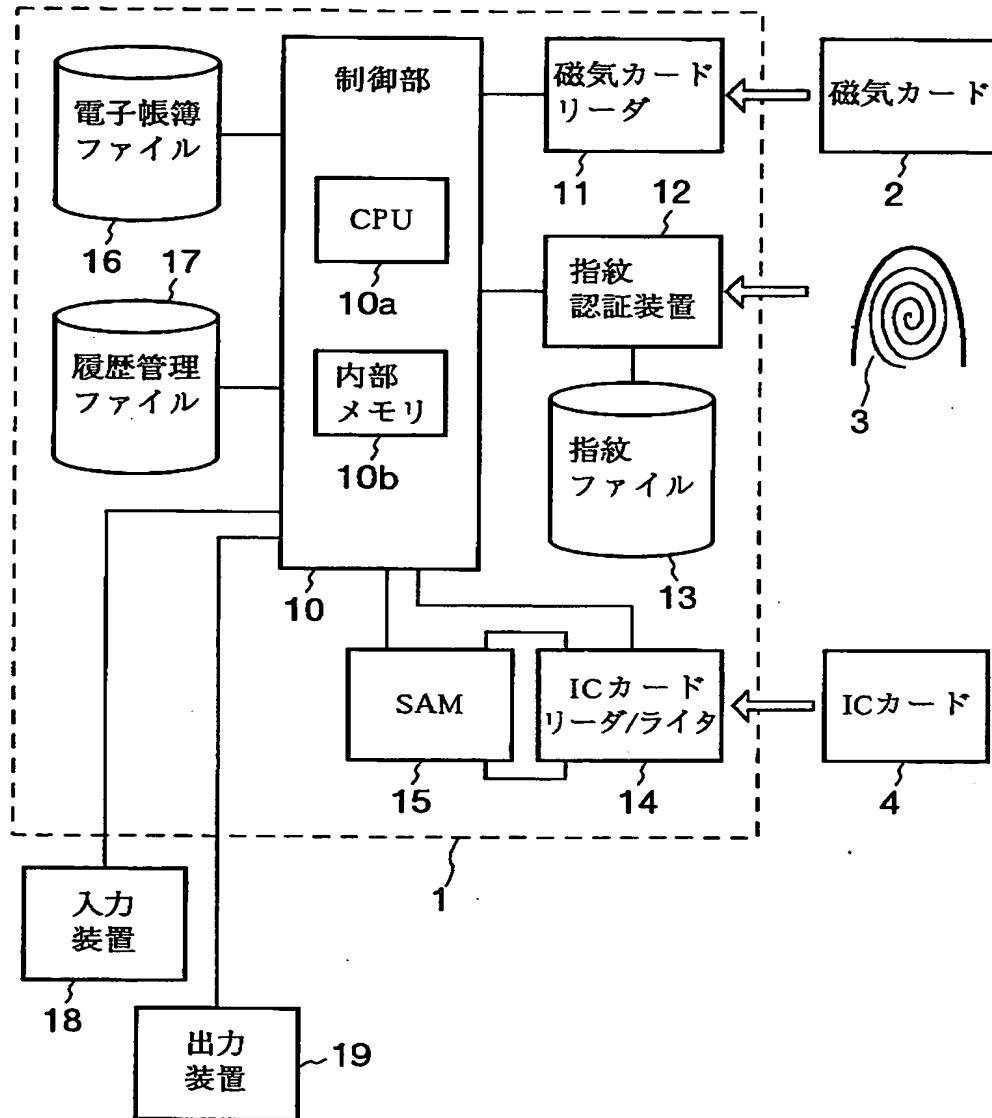
【符号の説明】

- 1 電子帳簿管理装置
- 2 磁気カード
- 3 指紋
- 4 ICカード
- 10 制御部
- 10a CPU
- 10b 内部メモリ
- 11 磁気カードリーダー
- 12 指紋認証装置
- 13 指紋ファイル
- 14 ICカードリーダー/ライター
- 15 SAM

- 1 6 電子帳簿ファイル
- 1 7 履歴管理ファイル
- 1 8 入力装置
- 1 9 出力装置
- 5 0 MOドライブ
- 5 1 MO
- 6 0 通信装置
- 6 1 ネットワーク
- 6 2 サーバ

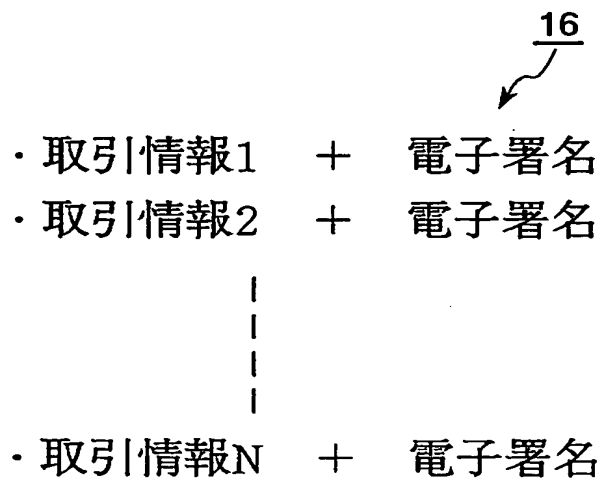
【書類名】 図面

【図 1】





【図 2】



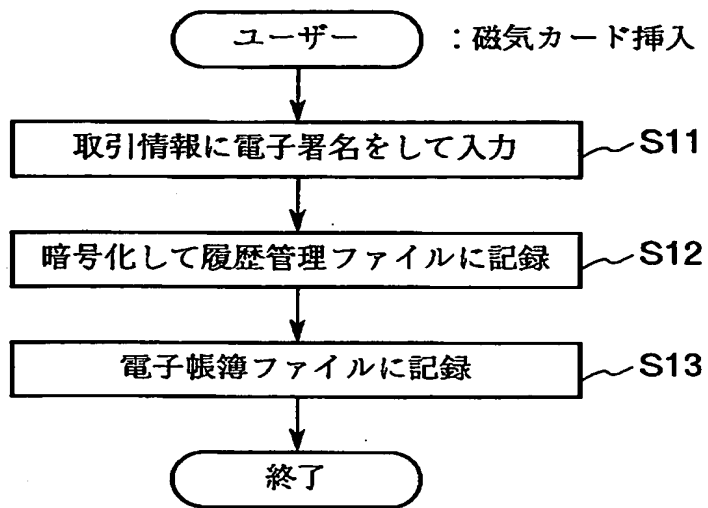
【図 3】

17

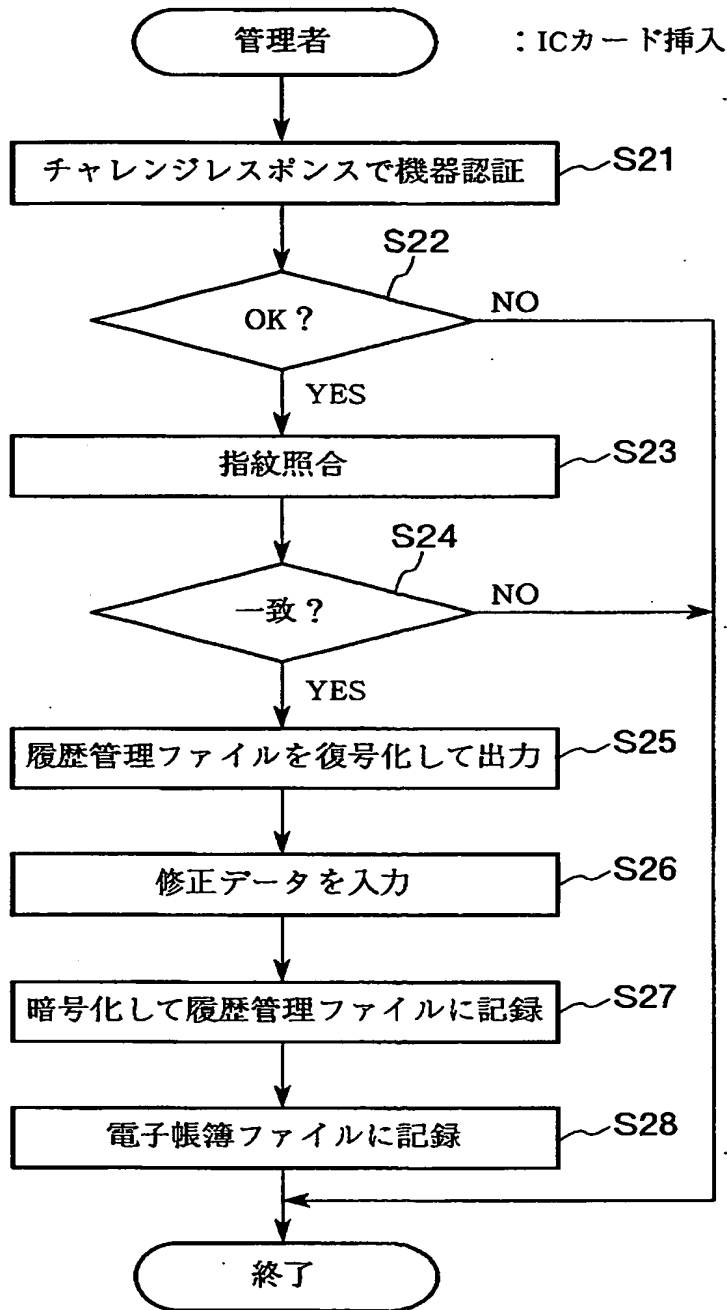
↓

日付	時間	利用者	利用内容	金額	正常終了?	修正?	修正内容
○月○日	XX:XX	①△△△	出金	10,000	○(電子署名)	無	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

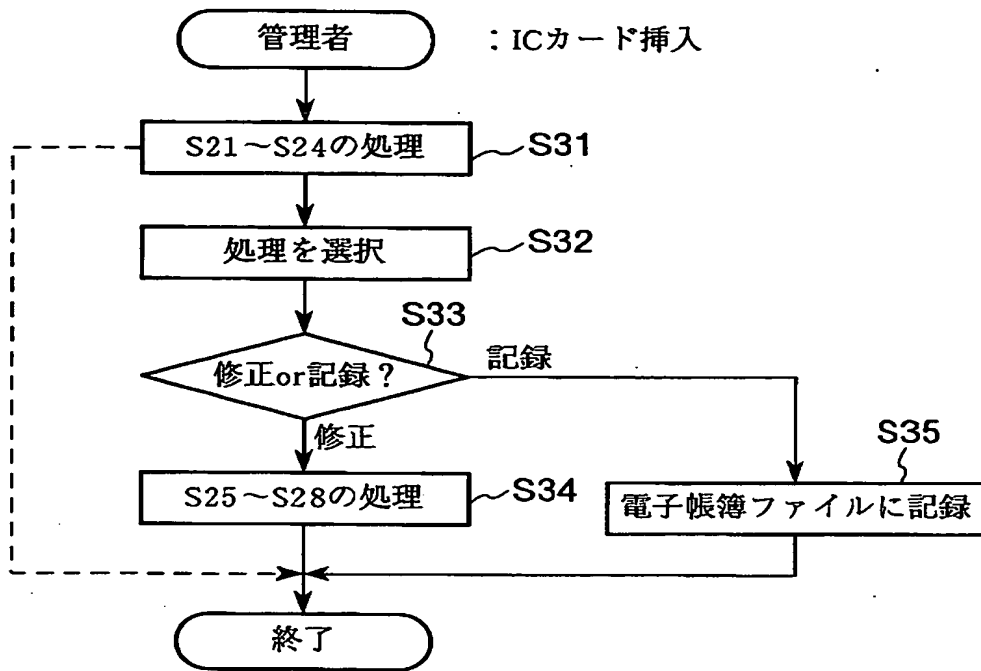
【図 4】



【図 5】

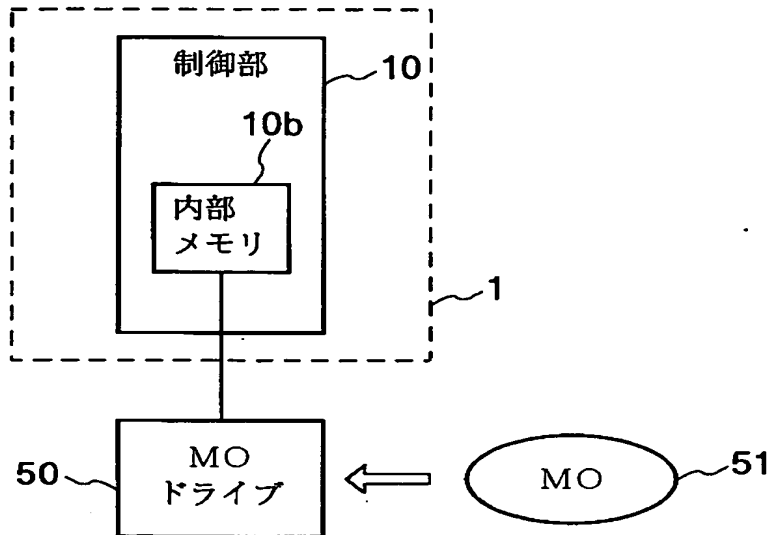


【図 6】

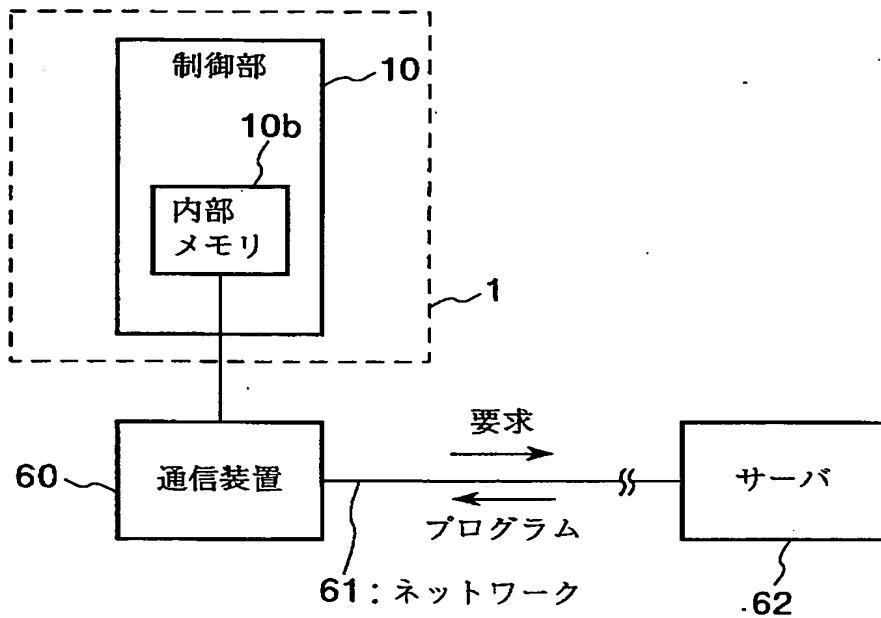


【図 7】

(a)



(b)



【書類名】 要約書

【要約】

【課題】 電子帳簿などの電子データの管理について、高いセキュリティを達成する。

【解決手段】 ユーザは、磁気カード2を磁気カードリーダー11に読み取らせ、電子署名と共に取引引き情報を入力装置18から入力する。この取引引き情報は、電子署名と共に電子帳簿ファイル16に記録され、暗号化されて履歴管理ファイル17に記録される。管理者は、取引引き情報を修正するとき、ICカード4をICカードリード／ライト14に挿入してSAM15との間で機器認証させると共に、指紋ファイル13に記録された指紋のデータと当該管理者の指紋3のデータとを指紋認証装置12に照合させる。機器認証、指紋の認証の双方が得られると、制御部10は履歴管理ファイル17を復号化し、電子帳簿ファイル16の修正を可能とさせる。そして、管理者が入力した電子帳簿ファイル16の修正に関するデータも暗号化されて履歴管理ファイル17に記録される。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000168285]

1. 変更年月日	1990年 8月 9日
[変更理由]	新規登録
住 所	山梨県甲府市大津町1088-3
氏 名	甲府日本電気株式会社